PROPOSED PLAN TO SURVEY THE VULNERABILITY TO PENETRATION OF CIA HEADQUARTERS

1. BADGE SYSTEM:

Vulnerability Factors:

a. Possibility of duplication and use without detection.

TEST: With ordinary commercial facilities make a badge and compare it with a bona fide badge. If there are noticeable points of difference, test it through use.

b. Possible lack of rigid scrutiny of all badges by guard.

TESTS: (1) Check the scrutiny of badges by exchanging badges of several persons and see if they are detected.
(2) Use a temporary badge after expiration date.
(3) Check guard observance of restricted use of different type badges.

c. Possible non-return of lost badges.

TEST: Check Physical Security lost badge records and procedure when badge is not recovered.

2. USE OF TELEPHONES:

Vulnerability Factors:

a. Discussion of classified information.

TESTS: (1) Tap telephones.
(2) Make calls and solicit classified information over phone.

b. Use of CIA phone for long distance calls to and from covert or semi-covert personnel.

TEST: Tap telephone.

c. Disclosure of identity of CIA personnel, offices, or phone numbers over telephone to outsiders.

TEST: Review and appraise security rules for phone operators on this subject. Test points which appear vulnerable by making calls from within and without Agency.

3. IDENTIFICATION AND RESTRICTION OF MAINTENANCE AND SERVICE PERSONNEL:

Vulnerability Factor:

a. Possible lack of adequate identification and supervision of CSA personnel, (carpenters, electricians, char people, etc.) telephone men, roving or relief guards, chauffeurs, etc.

TESTS: (1) Make actual entrances under these guises and determine how much supervision is afforded within offices.

(2) Check identification ...entials for adequacy.

4. IDENTIFICATION, RESTRICTION AND SUPERVISION OF VISITORS

Vulnerability Factors:

a. Possible lack of good records and system for checking visitors.
TEST: Examine and appraise records and system for checking visitors.

b. Possible lack of control or supervision of visitors after entrance.
TEST: Make actual visits and determine how much supervision or control is afforded.

c. Possible lack of good control or vantage by guard at entrance.
TEST: Survey each guard post and check entrance control at rush hours.

d. Identification of visitor from other agencies seeking classified information.
TEST: Make actual visit under cover of State or Defense and ascertain what checks are made by various CIA offices to assure identification prior to discussing classified information.

5. CONTROL OF APPLICANTS FOR EMPLOYMENT:

Vulnerability Factors:

a. Discussion of classified information with applicant in Personnel Office.
TEST: Make actual application and obtain interviews with Personnel.

b. Discussion of classified information with applicant by interested office upon referral by Personnel for interview.
TEST: Make actual application and obtain interviews with Personnel and other offices.

6. UNCLEARED POOL EMPLOYEES:

Vulnerability Factors:

a. Possible use on classified matter.
TEST: Check rules and procedures for use of uncleared pool personnel. Plant person in pool and arrange for absence and use in office with visitor pass and see if detected.

b. Possible absorption of classified information through outside contacts with future supervisor.
TEST: Question pool employee re contacts with future supervisors.

7. EXTRACTION OF CLASSIFIED MATERIAL FROM OFFICES:

Vulnerability Factor:

a. Possible withdrawal of classified papers in brief cases, envelopes, or packages.

TEST: Explore the feasibility and practicability of requiring passes for all hand-carried papers, brief cases and packages, or the institution of spot checks.
(Note: This would still not catch the material which could be taken out in pockets or hand bags.)

8. PENETRATION BY ELECTRONIC DEVICES:

Vulnerability Factor:

a. Possible installation of mikes, recorders or transmitters.

TEST: Survey of sensitive areas.

9. PHYSICAL PENETRATION THROUGH OTHER THAN ORDINARY ENTRANCES:

Vulnerability Factor:

a. Possible entrance through windows, basements, skylights, etc.

TEST: Physical survey.

10. PENETRATION THROUGH FALSE APPLICATION:

Vulnerability Factor:

a. Possible employment of enemy agent who has submitted PHS covering background of security acceptable person.

TEST: Check personnel and investigative procedures to ascertain whether such a false PHS would be detected.

POINTS OF POSSIBLE VULNERABILITY TO SECURITY COLLATERAL TO PENETRATION

1. OUTSIDE ACTIVITIES OF EMPLOYEES:

Vulnerability Factor:

a. Possible vulnerability to exploitation by enemy agent or others through loose talk.

TEST: Test suspected employees through association at places, etc. Post listeners in shuttle buses, cafeterias, medical waiting room, etc. Monitor agency pool cars.

2. FORMER EMPLOYEES:

Vulnerability Factors:

a. Possible unwitting exploitation.

TEST: Check adequacy of exit interview and emphasis on consequences for violations.

b. Possible open exploitation.

TEST: Explore possibility of requesting people leaving agency to advise us of any attempts at exploitation.

3. EMPLOYEES ORDERED OVERSEAS:

Vulnerability Factor:

a. Possible lack of adequate security indoctrination (employee and dependents).

TEST: (Extent of security indoctrination is now being explored.)

4. PROCUREMENT PROCEDURES:

Vulnerability Factors:

a. Possible inadequate security checks prior to discussion of classified matters.

TEST: Explore current procedures.

b. Possible inadequate security checks for those engaged in classified work.

TEST: Explore situation with view to compartmentalization and/or cut-outs.

5. HANDLING MAIL AND CABLES:

Vulnerability Factor:

a. Possible loose procedures.

TEST: Survey mail and cable handling.

6. POSSIBLE COMPROMISE OF COVERT PERSONNEL:

Vulnerability Factor:

a. Visits to CIA offices.

TEST: Check visitors' log against [illegible]rt files.

7. OTHER AGENCY LIAISON PERSONNEL:

Vulnerability Factor:

a. Possible personnel security risks in other agencies.

TEST: Check basis of security clearance of other agency personnel by CIA for its adequacy.

8. OTHER AGENCY SECURITY PRACTICES:

Vulnerability Factor:

a. Possible compromise of CIA classified documents in other agencies by lower security standards and practices.

TEST: Check present CIA restrictions on other agencies against practices.